	NORTH CAROLINA DEPARTMENT OF COMMERCE DIVISION OF WORKFORCE SOLUTIONS
	DWS POLICY STATEMENT NUMBER: PS 08-2017
	Date: April 4, 2017
	Subject: Electronic File Storage and Protecting Personally Identifiable Information
	From: *William H. Collins, Jr.* William H. Collins, Jr. Assistant Secretary for Workforce

Purpose: To provide guidance on the use of electronic file storage, protecting Personally Identifiable Information (PII) and retrieval of workforce and other federal funds' participant, program and financial documents; and to rescind Policy Statement No. 10-2014.

Background: Local Workforce Development Areas and the North Carolina Division of Workforce Solutions (DWS) must maintain many forms of documentation and data for federal funds purposes. These documents and data may be stored electronically and must have the ability to be retrieved as per guidance in this Policy Statement.

US Department of Labor (USDOL) Training and Employment Guidance Letter (TEGL) No. 39-11 provides additional "Guidance on the Handling and Protection of Personally Identifiable Information."

Action: Local Workforce Development Areas and DWS offices using electronic file storage and retrieval systems must meet the minimum requirements as outlined in Attachment I of this Policy Statement to maintain and protect information. Local Workforce Development Areas must also protect consumer Personally Identifying Information (PII) as outlined in Attachment II. Effective July 1, 2015, all WIOA Title I and Title III Wagner-Peyser participant and program related documents must be scanned in and stored in NCWorks Online. Attachment III outlines the processes and procedures that must be followed when scanning documents into the system. In addition to NCWorks Online data, all customer information must be protected as outlined in this Policy Statement and referenced TEGL.

DWS must use all preventive measures to ensure that the confidentiality and integrity of all PII remains intact. It is expected that all boards, their representatives and DWS staff will take necessary steps to protect PII data collected from individuals and employers. This includes redacting any unnecessary PII data when using for verification. Further, all PII data

collected for use in WIOA programs must comply with the state's Security Information Policy.

https://ncit.s3.amazonaws.com/s3fs-public/documents/files/SISM-2-2016.pdf

Effective Date: Immediately

Expiration: Indefinite

Contact: Field Services Program Staff

Attachment 1:   North Carolina Guidance for Workforce Innovation and Opportunity Act and Other Federal Funds Electronic Image Storage

Attachment 2:   North Carolina Guidance for Workforce Innovation and Opportunity Act and Other Federal Funds Protection of Personally Identifiable Information (PII)

Attachment 3:   North Carolina Guidance for Workforce Innovation and Opportunity Act and Other Federal Funds Scanning Procedures for Consumer Documents in NCWorks

ATTACHMENT I

NORTH CAROLINA GUIDANCE FOR WORKFORCE INNOVATION AND OPPORTUNITY ACT (WIOA) AND OTHER FEDERAL FUNDS

ELECTRONIC IMAGE STORAGE

At a minimum, Electronic Storage and Retrieval Systems must:
- Ensure the integrity, accuracy, authenticity, and reliability of the records kept in an electronic format;
- Be capable of retaining, preserving, retrieving, and reproducing the electronic records;
- Be able to update/convert the records as new technology develops;
- Organize documents in a manner consistent with applicable Division of Workforce Solutions policies;
- Ensure that financial and program records maintain a completeness of documentation, are organized by Program Year, and are sufficient for a complete audit trail;
- Have adequate disaster recovery plans, including proper anti-virus protection, tamper proof secondary/supplementary data storage facilities such as regular backup in an external hard drive, and stored in a safe location;
- Ability to convert paper originals stored in electronic format back into legible and readable paper copies; and
- Have adequate records management practices in place.

Before implementing the use of an Electronic Storage and Retrieval System, the following requirements must be met by the Local Workforce Development Area:
1. Electronic Data Storage and Retrieval Policies, Procedures and/or Guidelines in place that adhere to all federal, state, and local laws and policies governing the use and storage of electronic data.
2. Adequate computer hardware necessary for implementation, including scanners.
3. Appropriate electronic document storage and retrieval software to include capacity to scan and retrieve documents in universally accepted file formats such as PDF.
4. Adequate organization server storage capacity which complies with record retention and access regulations as outlined by the Workforce Innovation and Opportunity Act, Public Law 113-128, Section 185.
5. Adequate security measures, for example, password protected assigned access.
6. Documented compliance with vendor recommendations regarding security and login identification and conformity with all software vendor licensing guidelines.
7. Appropriate licensure for software including adequate user licenses as recommended by vendor.
8. Appropriate archiving procedures for storing outdated and/or no longer useful documents.
9. Access capability for DWS and federal officials for data validation, monitoring, and auditing as needed.
10. A notification system to contact impacted individuals if data is compromised.

ATTACHEMENT II

NORTH CAROLINA GUIDANCE FOR WORKFORCE INNOVATION AND OPPORTUNITY ACT (WIOA) AND OTHER FEDERAL FUNDS

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Each Local Workforce Development Area must take all necessary precautions to protect the Personally Identifiable Information (PII) of consumers. USDOL Training and Employment Guidance Letter (TEGL) No. 39-11 gives the following definitions and information related to PII:

- Personally Identifiable Information (PII) – Federal Office of Management and Budget defines PII as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. [1]

- Sensitive Information – any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.

- Protected PII and non-sensitive PII - the U.S. Department of Labor has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

  1. Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, Social Security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse name, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

  2. Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, email addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

  To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a Social Security number, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

TEGL 39-11 lists a number of requirements that must be followed by all grantees to ensure the protection of PII including taking the steps necessary to protect the data from unauthorized disclosure. In addition, the appendix of TEGL 39-11 lists a number of federal laws related to data privacy, security, and protecting PII. These laws need to be reviewed and followed by each local Workforce Development area in order to fully protect consumer PII from being inappropriately

disclosed. Local Areas need to make sure they stay abreast of current federal, state, and local legislation pertaining to privacy and security of consumer data.

When uploading verifying documentation in NCWorks Online, be sure to redact protected PII that, if disclosed, could result in harm to the individual whose name or identity is linked to that information. At a minimum all instances of an individual's driver's license and the first five digits of the SSN must be redacted. Please consult the scanning procedures in Attachment III of this document for specific information on how to redact information in NCWorks. NC General Statute 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit or special identification card..." When scanning driver's licenses and social security cards into NCWorks, please be sure that all images are in grayscale.

No PII data that is loaded into the state's NCWorks Online system should be stored or transferred on any portable devices. This includes laptops, tablets, mobile phones, thumb drives, CDs or other similar devices that are not protected by "Encryption Technology" (North Carolina Statewide Information Security Manual section 0401002).

[1]OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)

ATTACHMENT III

NORTH CAROLINA GUIDANCE FOR WORKFORCE INNOVATION AND OPPORTUNITY ACT (WIOA) AND OTHER FEDERAL FUNDS

SCANNING PROCEDURES FOR CONSUMER DOCUMENTS IN NCWORKS

In order to ensure consistent consumer information is entered in NCWorks and case files are as complete as possible while still ensuring the protection of consumer personally identifiable information (PII), the following processes and procedures must be followed when scanning documents into the system.

- NC General Statute 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit or special identification card..." All documents that are scanned into NCWorks will be scanned in grayscale.

- In addition to the items outlined in NCGS 20-30, any document that would pose an identity theft risk to the individual if stolen should not be scanned in color. This includes but is not limited to the following: social security cards, passports, and birth certificates.

- Each document must be reviewed carefully prior to scanning to identify all items needing redaction. At a minimum, all instances of the driver's license/identification number and the first five digits of the social security number must be redacted.

- Verify that the documents are complete before scanning. Signature pages should not be scanned separately from the core document. Examples: Applications/intakes, Individual Employment Plans (IEPs), and Individual Service Strategy (ISS) documents.

- Documents must be scanned as separate files into the system rather than as one electronic file containing all of the consumer's records. This includes scanning identification documents such as the driver's license and social security card separately.

- Document tags and, where possible, filenames must be clear so that it is obvious what each document in the file list is prior to opening it. Use of a standardized naming system within the board is encouraged.

- After scanning/uploading documents into NCWorks Online, use the 'redaction tool' found in the "Create Annotations" toolbar to draw a shape over information that needs redacting. Before saving the altered image, make certain you have chosen under the "Annotation Options" to make the redaction a "Separate layer that can be changed later". Do NOT try to redact information PRIOR to loading it into NCWorks Online.

- The contents of the electronic file in NCWorks Online should be identical to the hard copies (or originals) used by staff to capture the information electronically. If a document is updated, such as the IEP or work experience agreement, the entire updated document must be scanned into the system as a separate file. Once documents are preserved in NCWorks Online, when appropriate, their originals should be securely destroyed to further protect customers' information.

- Once in NCWorks, redacted information must be completely unreadable unless the user has the proper permissions to remove the redaction. As stated in Attachment I, DWS staff and federal officials need to have the ability to access redacted information for data validation, monitoring, and auditing purposes. Therefore, redaction should be done in NCWorks ONLY so that the ability to convert paper originals stored in electronic format back into legible and readable paper copies remains.